U-4 2-6

14-6

~~TOP SECRET~~

87

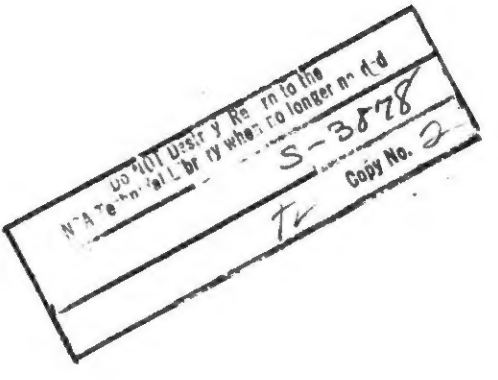
ARMED FORCES SECURITY AGENCY

92/50/TOPSEC/AFSA-14

Copy No. 6

From: AFSA-14

To: AFSA 02 A7



~~TOP SECRET~~

DF 187-F 92/50/TOPSEC/AFSA-14

REMARKS MADE BY MINISTERIALRAT FENNER IN REPLY TO CERTAIN QUESTIONS OF A GENERAL NATURE

1. During his period of detention (September-December 1946) at the Hq 7707 European Command Intelligence Center, Oberursel, Germany, Wilhelm FENNER, former Ministerialrat and chief of cryptanalysis in the Armed Forces High Command Cryptologic Agency (OKW/Chi), wrote a lengthy report concerning his past career and his extensive experiences in the field of cryptology. This report was never issued in translation although an inadequate summary by Army Security Agency was issued as TICOM/I-206.

2. The present DF 187 Series will constitute, when completed, a translation of FENNER's entire written report. The attached is the seventh and penultimate of the series and contains FENNER's remarks made in reply to certain questions of a general nature. Because the questions cover a wide range of topics without specific relation to one another, no attempt has been made, as in previous issues of FENNER's answers, to make of the report an integrated whole. Within this report the questions with their answers have been included as separate and distinct items, although some thought has been given to their logical arrangement. Pertinent notes from the TICOM files and from the memory of one of FENNER's original interrogators, MARY C. LANE, Capt. WAC, have been added.

3. Previous TICOM reports of this series are:

DF 187	The Career of Wilhelm FENNER with Special Regard to his Activity in the Field of Cryptography and Cryptanalysis
DF 187-A	Organization of the Cryptologic Agency of the Armed Forces High Command, with Names, Activities, and Number of Employees together with a Description of the Devices Used
DF 187-B	The Cryptanalytic Successes of OKW/Chi after 1938
DF 187-C	Relations of OKW/Chi with Other German Cryptologic Bureaus
DF 187-D	Relations of OKW/Chi with Foreign Cryptologic Bureaus
DF 187-E	Comments by FENNER on the Austrian Cryptologic Bureau and Former German Colleagues

August 1950 35 copies

Translated: RWP 53 pages

Edited: MCL

INDEX OF QUESTIONS

QUESTIONS		PAGES
1.	What have you done from May 1945 to the time of your arrest? Have you been in contact with your former associates? If so, how have you been in contact with them? Do you know what has become of your former associates? How did you learn such details?	7
2.	Give an account of the history and organization of Reichswehrministerium Cryptologic Bureau; personalities in it. What continuity was there with the 1918 organization? When did the German Defense Ministry (Reichswehrministerium) become the German War Ministry (Reichskriegsministerium) and what was the difference between the two organizations?	10
3.	Did the NSDAP exert any direct or indirect pressure on OKW/Chi?	11
4.	Did you know of, or suspect, the presence of Gestapo or other Party agents in your organization? Did you feel that you and other competent experts had a free hand in planning and executing your tasks?	14
5.	What, in general, did OKW/Chi have to do with the Abwehr?	16
6.	What cooperation existed between OKW and Abwehr intercept units?	18
7.	What cryptanalytic work was attempted by the Waffen-SS?	18
8.	What do you know about the work of agents? How was the work set up and handled, as for instance, in the Referat Vauck?	19
9.	What was your opinion of the papers circulated by SCHAUFFLER in the Auswaertige Amt? Did you ever contribute to these papers?	21
10.	What can you tell about German General Staff Intelligence Studies on Russia? What agencies existed for the gathering of material for the intelligence studies, who composed the personnel, and what was the product of their work? Were publications of such agencies distributed generally to cryptographic or cryptanalytic units?	21
11.	What do you know about the Russian signal intelligence organization? Did the Germans have any contact with the Russians, White or Red?	22
12.	What was published by the Germans concerning Russian order of battle? By whom was it published and when? Are there any copies to be found?	22

QUESTIONS		PAGES
13.	Did OKW/Chi keep a list of terms of Russian mechanized equipment, guns, planes, etc.?	21
14.	Are any atlases and maps of Russia available? What sort were available and by whom were they prepared?	22
15.	What was the procedure with German patents on communications equipment? Were there any "secret" lists of such patents? Where would they be now?	23
16.	Do you recall any leads or ideas of American, British, or other nationality patents which were important to the work of OKW/Chi?	24
17.	Do you know the names of any American, British or Russian cryptologists?	25
18.	Do you know of any cryptographic organization of public character in Europe? If so, what were the names and locations of such societies? Do you know the names of any members?	28
19.	Give an account of your liaison with the Japanese nationals NISHI and SAKURAI.	28
20.	What use did cryptanalysts make of OKW/Chi library and archives? How were reference materials such as news broadcasts made available to cryptanalysts? What were the reference materials available? Where are they now?	31
21.	Did OKW/Chi keep a list of abbreviations, of terms of standard translation or special phrases? Where is this material now?	32
22.	What dictionaries were used by OKW/Chi? Are any now available? Describe the work done by Sdf. KUEHN on military dictionaries.	33
23.	Do you feel that information produced by the crypt-analytic people was properly handled? Who evaluated the information? How and to whom was it disseminated? What did the recipients do with it?	34
24.	Describe the preparation, selection of material, publication, translation, and distribution of the VNs.	35
25.	Describe the training which should be given to a cryptanalyst. What are the basic requirements for a good cryptanalyst?	41

DF 187-F

REMARKS MADE BY FORMER MINISTERIALRAT FENNER IN REPLY TO CERTAIN QUESTIONS OF A GENERAL NATURE

1. What have you done from May 1945 to the time of your arrest? Have you been in contact with your former associates? If so, how have you been in contact with them? Do you know what has become of any of your former associates? How did you learn such details?

In May 1945 I was in Werfen where the railway train with the remnants of Chi was standing at the station. My activity consisted in eating, drinking, taking a walk, chatting with my people. As far as my people knew foreign languages they were assigned as interpreters because there was a great deal to do. Since at that time there were occasional wild rumors about the setting up under American command of German units to fight against Bolshevism, I twice contacted the adjutant of Combat Group Bork (at the time that was the tactical unit to which we were subordinated), in order to suggest in such case the advisability of taking over all my people as a group. Furthermore some of my people asked me for a letter of reference. I wrote one for MENZER.[1]

Toward the end of May the remnant of Chi was transferred by the Americans to Heufeld in Upper Bavaria. I spent my time there by writing letters of reference for all former members of my unit who were then present; Ministerialrat Dr. WENDLAND[2] and Regierungsrat Dr. WEISSER[3] assisted me in this. Early in June I was transferred to the "Fuehrerreserve", i. e., after the release of civilians there now began the successive release of officers and officials with officer rating according to a plan approved by the Americans. I went to Bruckmuehl on the Mangfall (Upper Bavaria) and was obliged to wait without any activity until I should be taken away to a prison camp. That happened about 18 June 1945. With most of my comrades I came to Landshut. Originally

---

1. [illegible] experts in German cipher machines, later interrogated by US authorities. See DF 174. [Ed. Note]

2. Interrogated by TICOM in 1947. See TICOM/I-202.

3. Interrogated by TICOM in 1947. See TICOM/I-201.

DF 187-F

I wanted to go home to the Russian Zone of Occupation, to Hangelsberg on the Spree where I had left my wife, but American officers warned me against doing so. I was therefore undecided as to what I ought to do. Then by chance I became acquainted in the camp with the new Landrat of Kreis Mallersdorf, Herr HARTENBACH, who wrote me a recommendation to the new Landrat of Kreis Straubing in Lower Bavaria, Herr BICKLEDER. I was released on the 19th or 20th of June 1945 and went to Straubing where I arrived 21 June and had a room assigned me by the housing office at the home of merchant VEIT, Hindenburg-strasse 18. The Landrat had no possibility of using me, however, although it was not my non-membership in the NSDAP which was decisive but, as I was told, because I could not "be employed in the public service as a matter of principle since I was a high official of the former German "Wehrmacht". Since I had money enough to get along for a few weeks I went for a walk. And as I walked I was in excellent spirits because during the entire war I had never had more than three days leave at a time. I also was hungry. Between the beginning and middle of July 1945 I applied to Justizrat Dr. PRAGER for advice because my idleness was gradually becoming distasteful. PRAGER gave me a recommendation to the Regierungspraesident in Regensburg, Dr. FALKNER. I found him at the home of the architect, SCHMID. But when FALKNER heard that I had been in the War Ministry and therefore automatically in OKW up to the time of my transfer to General der Aufklaerung Sued,[4] he declined to intercede for me on the grounds that they only had room for Bavarians. I then went to the Labor Office and had to clean up a house at Pandurengasse which had been badly damaged by an air attack. Later I spent weeks sawing and splitting wood on the same property; I picked out all sound beams and piled everything in order on the ruined site. Late in September I went to Heidelberg to try to

[illegible]nnection with the industrialist HANNEMANN whom I knew by name.

---

4. During the closing days of the war the German Army signal intelligence forces were divided into northern and southern groups. FENNER here states he was assigned to Army Signal Intelligence South. [Ed. Note]

DF 187-F

But HANNEMANN was away and I returned to Straubing at once. There I had meanwhile become acquainted with Max KNOEDL who ran an automobile repair and sales business. He took a liking to me and suggested that I work in his workshop. I could not start at once, however, because there were two conditions which had to be fulfilled: I declined to work with Georg HESSLER who was the boss in the shop because he did not make a good impression on me and because he had been a Party member; also the Labor Office would have to assign me to KNOEDL. So I continued sawing and chopping wood. As of 1 December 1945 I was assigned by the Labor Office to the KNOEDL Firm as helper and continued to work there as mechanic on bicycles and automobiles until the time of my arrest on the evening of 2 July 1946. I carried stones to build a house, helped dig a well, excavated for a foundation, and evenings took account of stock, prepared the weekly account showing receipts and expenditures, and made myself useful about the premises wherever necessary.

The question, with what members of the cryptologic organization I have been in contact since the war, is probably to be construed to mean, with what former members of Chi I have been in communication after the war was over. These persons are:

1. Frau Ilse SCHWAB,[5] wife of Dr. Jur. Kurt SCHWAB. Frau SCHWAB worked for me in the Telegram Registry of Chi and during the last months before the evacuation of Berlin sometimes helped me in the secretariat. She came with me to Straubing, worked first as clerk at KNOEDL's and then found a position at the airfield in Straubing, working for the Red Cross.

2. My sister Mathilde FENNER.[6] I have written her two private letters; she may have written me three. You can learn her address through my sister Frau Dr. Johanna MICHAELSSON, Schoenberg, Kreis Calw in Wuerttemberg, French Zone.

---

5. See DF 187-A, p. 5, where Frau Ilse SCHWAB is entered as a member of the Section, Registry of Telegrams, Group a, Main Group B, OKW/Chi.

6. See DF 187-A, p. 7, where Frl. Mathilde FENNER is entered as a member of Section 5 (France, Belgium, Netherlands, Switzerland, Egypt), Group b, Main Group B, OKW/Chi.

DF 187-F

3. Herr MORS, British Zone (address unknown to me)[7] wrote me a card late in 1945 informing me that he had opened a translation bureau. I did not answer him.

4. Herr MENZER,[8] apparently an automobile mechanic in Zschoppau, Saxony, Russian Zone, wrote me a postcard and told me that he was trying hard to become a competent person in his new calling. I did not answer him.

5. Frl. Gertrud BAULE[9] told me in the fall (?) of 1945 on a form postcard that she had either become engaged or married. I do not quite recall. I did not answer.

6. Herr SCHNELLBACH[10] from Regensburg notified me on a printed card that he had married. I did not answer. His wife is the former employee OSTERODE, who last worked in the archives with Dr. SCHAEDEL. (I omitted her name there because I did not recall her).[11]

7. First Lieutenant Otto KUNZE[12] wrote me about the middle of April from a prisoner-of-war camp in Garmisch-Partenkirchen that he was the only one who had not yet been released. I did not answer him.

---

7. See DF 187-A, p. 7, where Angestellter Robert MORS is entered as a member of Section 6 (England, USA), Group b, Main Group B.

8. See DF 187-A, p. 4, where Reg. Oberinsp. Fritz MENZER is entered as a member of Group I, Main Group A.

9. See DF 187-A, p. 8, where Frl. Gertrud BAULE is entered as a member of Section 11 (Greece), Group b, Main Group B.

10. See DF 187-A, p. 6, where Corvin SCHNELLBACH is entered as a radio operator in Section 4 (Italy), Group b, Main Group B.

11. See DF 187-A, p. 11, where it is stated that Dr. SCHAEDEL was assisted in the archives by "three female employees and one enlisted man".

12. See DF 18[illegible] [illegible]t. Otto KUNZE is entered as leader of [illegible]

DF 187-F

8. Frl. Irmgard KOEPP,[13] now in Regensburg, Reichspost, Military Directorate, twice visited my wife in Straubing. I exchanged a few words with her.

Those are my contacts with the former members of my old unit. From Frl. KOEPP I also heard that Colonel KETTLER[14] is supposed to be active in an insurance agency and that HUETTENHAIN[15] is supposed to be in London. What has become of the other people I do not know. It is possible that:

Freifrau von MEDEM is in Bad Aibling,[16]

Frl. Dr. BRUSSOW is in Weihenkirchen,[17]

Frau BENNINGHOVEN is in Weihenkirchen,[18]

Dr. Franz WEISSER is in Bruckmuehl,[19]

All these places are in Upper Bavaria.

---

13. See DF 187-A, p. 7, where Frl. Irmgard KOEPP is entered as a member of Section 6 (England, USA), Group b, Main Group B.

14. Chief of OKW/Chi in 1944 (DF 187-A, p. 3). Compare DETMANN's statement (DF 185, Part II, p. 110) that KETTLER had been Director of an Information Office in Hamburg, but since 12 August 1947 was director of a bureau in Munich (Address: Muenchen, Isabellastr. 29 b/Opitz). MENZER states that he addressed a letter to KETTLER at this address (DF 174, p. 14) but received no answer.

15. See DF 187-A, p. 11, where HUETTENHAIN is entered as head with FENNER and WENDLAND of Section 4 (Training and Instruction), Group C, Main Group B. See DF 185, Part I, p. 98, note 1 for references to HUETTENHAIN in TICOM interrogation reports.

16. See DF 187-A, p. 5, where Freifrau Edith v. MEDEM is entered as a member of the Section Registry of Telegrams, Group a, Main Group B.

17. See DF 187-A, p. 7, where Frl. Dr. Margarethe BRUSSOW is entered as a member of Section 6 (England, USA), Group b, Main Group B.

18. See DF 187-A, p. 7, where Frau Anne BENNINGHOVEN is entered as a member of Section 6 (England, USA), Group b, Main Group B.

19. See DF 187-A, p. 7, where RR Dr. Franz WEISSER is entered as a member of Section 6 (England, USA), Group a, Main Group B. See also TICOM/I-201 "Interrogation of [redacted] Phil. Studienassessor of Anglo-American [redacted] states that he was in Bruckmuehl as private tutor from June 1945 to 1 May 1946 when he went to Augsburg as teacher of Latin, German and French in the Oberschule at Augsburg. WEISSER's daughter (ill with tuberculosis) remained in Bruckmuehl.

DF 187-F

2. Give an account of the history and organization of Reichswehrministerium Cryptologic Bureau; personalities in it. What continuity was there with the 1918 organization? When did the German Defense Ministry (Reichswehrministerium) become the German War Ministry (Reichskriegsministerium) and what was the difference between the two organizations?

In the First World War there was no cryptologic bureau. Cryptanalysis was carried on at Grand Headquarters, in some Armies, and also with a Bavarian Army Corps. The Cryptologic Bureau of the German Ministry of Defense (Reichswehrministerium) was founded in 1921. Its spiritual founder was First Lieutenant BUSCHENHAGEN who had been for a time during the war liaison officer stationed with the Austrian cryptanalytic unit in Bozen (Tyrol). BUSCHENHAGEN organized a small new cryptanalytic section and had among his personnel two employees who had done such work during the World War. These were the employees Hellmut MUELLER and Nikolai ROHEN, who later became officials in the Cryptologic Agency of the German Armed Forces (OKW/Chi). All the other personnel were new.

During some one of the frequent Communist disturbances, BUSCHENHAGEN succeeded in rescuing from bundles of documents which had been partially plundered about 100 reports of the former cryptanalytic unit. These were mostly reports from Headquarters and from the Bavarian cryptanalytic unit. This material I worked through and put in order when I was trying to ascertain what kind of cryptographic systems had been used and solved during the First World War.[20] From these reports I later prepared some 55 documents each about five centimeters thick. When we had to count on Berlin's being directly endangered, this material was taken to Jueterbog to the artillery barracks and was either destroyed there or fell into the hands of the Russians. During the last months other transfers of old documents were made which were withdrawn from my control because I had nothing to do with them. Therefore it is possible that this material was not known to me.

20. This is the material to which reference is made in the history of the Cryptologic Agency which is probably to be attributed to FENNER: "In the spring of 1919, supposedly over the protests of Red contemporaries, he (BUSCHENHAGEN) succeeded in rescuing from the mass of documents of the Chief Signal Officer what turned out to be extremely valuable basic materials - primarily cryptanalytic reports, the study of which contributed in later years to the recovery without great expenditure of energy of forgotten experience". (DF 202, p. 6).

DF 187-F

I believe the German Defense Ministry (Reichswehrministerium) became the German War Ministry (Reichskriegsministerium) after the introduction of universal military service. The exact day I do not know. In almost any old German pocket calendar, however, you will find on one of the last pages a number of notes on "Nationally Noteworthy Days." The exact date can be looked up there without difficulty. The U.S. War Department doubtlessly has a collection of German laws. In the "Allgemeinen Heeresmitteilungen" the change of name must surely have been given and, of course, in the daily press. The change of name was made either by a decree of the cabinet or perhaps by an order of HITLER. In reality, the change of name was absolutely insignificant; it merely meant printing new letterheads, but in popular parlance the new Army (Reichsheer) continued to be called the "Reichswehr" despite its new name. In the language of the politicians the word "Wehr", taken critically, meant naturally merely defense while the word "Krieg" naturally contains the two concepts: defense and attack. How unimportant such designations are is shown by the fact that other countries likewise have called their Ministry of War a Ministry for National Defense without having any idea of indicating thereby that the country, as a matter of principle, is thinking only of defense. However, internal political considerations turn the scale in the choice of such official designations. Moreover, it is impossible to set up the claim that a country which calls its highest political authority a Ministry of War is merely on that account thinking aggressively. A modern example of this is France where the great mass of the population before this war was thinking defensively, indeed so defensively that even the military literature of their own country was occupied with this theme.

Between these two organizations there was no difference.

3. Did the NSDAP exert any direct or indirect [illegible] on OKW/Chi?

The Party, purely as a Party organization, naturally did not control OKW/Chi at any time. For this purpose they took other courses and employed other means. And this control was never directed against Chi as such but only against certain exponents. The controlling organ may always have been the competent Gestapo office or the Security Service (Sicherheitsdienst - SD)

DF 187-F

insofar as GOERING's "Research Bureau" (the Forschungsamt - FA) did not have a finger in the pie.

The following cases are known to me.

About April 1934, possibly even earlier, there was a check by the Forschungsamt on the gentlemen in the German War Ministry by means of telephone tapping. An eavesdropped telephone conversation of REICHENAU, at that time Chef des Ministeramts was direct occasion for the suicide of SCHIMPF. When Chi in respect to the cost of representation was still Group II of the Abwehr (while in respect to personnel and equipment it was subordinate to the Army Signal Branch (Inspektion der Nachrichtentruppen) under FELLGIEBEL)) the Forschungsamt had fitted out the desk telephone standing in the office of the Chef der Abwehrabteilung, Naval Captain PATZIG, with a device which permitted the Forschungsamt to listen in on conversations conducted in his room.[21]

About the same time there were numerous complaints by officers and officials of the Ministry regarding opened letters.

My mail sent me by my brother-in-law in New York was controlled and the Gestapo Control Office in Frankfurt/Oder informed me that a book addressed to me had been confiscated. The book was one which was much talked about

---

21. Compare FLICKE's statement (DF 116-AL, p. 9) "It had meanwhile been learned that various officers of the Department of Defense and of other military agencies had been under the surveillance of organs of the Forschungsamt and that their telephone conversations had been listened to. This caused bitter feeling. The Cipher Bureau was instructed to ascertain which telephone instruments were being tapped and in which rooms were located the microphones which had been installed in connection with repair work. It was learned that BECK, FRITSCH, and even BLOMBERG were being spied on in this fashion." In the same document FLICKE states that on the final evening in Oberhof (location of a war game in January 1934 at which SCHIMPF was present as an observer) SCHIMPF felt impelled to recite a little poem which he had written himself and which began with the words:

"If half in earnest, half in jest,
'Tis said we spy on you with zest,
Believe our honest face, I pray;
In general that is not our way."

DF 187-F

at that time. I have forgotten the title and also the author. That was about 1934. About 1937 State Secretary (Staatssekretaer) KOERNER in the Air Ministry demanded by immediate dismissal on the basis of a complaint raised by the Forschungsamt. One of my employees had stated that I had reviled GOERING in Russian. This employee was an agent of the Forschungsamt and reported to it whatever he might learn.

About the same time a former employee of Chi who later went over to the Forschungsamt (not in the first big group) kept inquiring of me about the status of the French section's cryptanalytic work. However, it is possible that he kept the results of his inquiries to himself because it was proven later that he had been a French agent. SCHAPPER[22] complained to Admiral CANARIS[23] about me with the aim of crowding me out of my position because he maintained I was disturbing the good understanding between the Forschungsamt and Chi. To the Ministry it was clear that this attack was intended merely as a prelude to a renewed attempt to dissolve the Cryptologic Bureau. The aversion to me may have been of a purely personal nature but the attacks on my person were in reality directed against the Bureau for I had no personal connection whatever with the Forschungsamt.

In 1944, long before the attempt on HITLER's life,[24] General THIELE told me I should be very cautious about telephoning even in my house in

---

22. SCHAPPER had been with OKW/Chi since 1929, having served in World War I in the intercept service. He had been entrusted with the organizational side of the intercept set-up for OKW/Chi in Berlin and became the "right-hand man" for SCHIMPF in the Forschungsamt in all matters of technique and organization. At the end of the war SCHAPPER was the head of the Forschungsamt with rank of Minister Director. For a biography of SCHAPPER see Appendix III of Volume 7 (GOERING's "Research" Bureau) of the 9-volume TICOM history "European Axis Signal Intelligence in World War II".

23. Chief of the Abwehr after 1935.

24. 20 July 1944 in which Generals Erich FELLGIEBEL and Fritz THIELE were implicated and on account of which they met death. THIELE was then Chief of Signal Command Section of OKW; FELLGIEBEL was Inspector General of Signal Troops of the Army.

DF 187-F

Hangelsberg because I must count on my phone (with secret number!) being watched. Packages which I received were opened at that time. However, it was definitely an official matter when the Forschungsamt failed to turn over the desired telegraphic traffic in spite of repeated requests. This went so far that from 1944 on requests for definite material were made only in very rare cases because the answer to be expected would turn out negative. Colonel KETTLER will confirm this.[25] Whatever else the Forschungsamt wished to learn regarding the accomplishments of Chi it probably heard through the Foreign Office. When after 20 July 1944 the State Security Main Office (Reichssicherheitshauptamt - RSHA) pushed itself into the foreground and the old Abwehr practically ceased to exist, contrary to expectation a certain relaxation of tension ensued. And I am of the opinion that after SS-Brigadefuehrer SCHELLENBERG[26] took over official duties, everything was dropped which looked like an effort to control Chi. For to the Militaerisches Amt, insofar as SS-Men had newly come into positions there, the entire military apparatus was so new that they would have found any control by any Party organs or their agents extremely disturbing.

And although Chi had long since ceased to be organizationally subordinate to the Abwehr nevertheless a complaint to SCHELLENBERG would have been sufficient to have the matter investigated and to have any control by outsiders and unauthorized parties stopped, in particular any control by the Forschungsamt, which according to a statement of SCHELLENBERG was to be dissolved just as certainly "as the Amen follows the Lord's Prayer in church".

4. Did you know of, or suspect, the presence of Gestapo or other Party agents in your organization? Did you feel that you and other competent experts had a free hand in planning and executing your tasks?

Among non-National Socialist officers and officials it was considered the rule that among three persons who were unknown to you at least one was an

---

25. Chief of OKW/Chi from 1 October 1943 to end of hostilities.

26. Head of Amt VI of the RSHA, who took over the Abwehr as the Militaerisches Amt of Amt VI of the RSHA.

informer. Naturally such persons were very hard to spot because they operated under their cloak of anonymity. At Chi it was only once possible to unmask a confidential agent of the Forschungsamt. When an opportunity offered, this person was then transferred. If word got around that any person in high position had been arrested, then the decent supervisors admonished their people to be very cautious. In my case it often happened, for instance, that General THIELE took me aside after a lecture and admonished me not to let fall any unfavorable criticism of the political system and of HITLER; comrades and subordinates who feared their superior might have made any incautious utterances also came and begged the man, for the sake of all decent co-workers, not to risk his head to no purpose. So there was really a constant, secret struggle of the opposition against the Party and certain officers who were marked as mixed up in Party politics. Within my own unit I always had the feeling that I had a free hand in respect to the work. Never did one of my associates rebel or assume an attitude of opposition. Even the few Party members among the officials and reserve officers were absolutely dependable since their National Socialism had virtually nothing in common with the type displayed publicly. In judging this question it must not be forgotten that my subordinates and superiors could see quite clearly from the VNs[27] what the truth really was. Consequently in my conferences I could allow myself much freedom, since once a week SCHAEDEL[28] gave a situation report based solely on secret information available to Chi and in which therefore the press of the various countries was left out of account.

Nevertheless it is possible that even among my personnel there were some people who were taking note of my words in order to use them to my disadvantage, if there was a chance. However, I would not be able to name any specific person.

---

27. Verlaessliche Nachrichten (Reliable Reports) - the name given to OKW/Chi decrypted messages.

28. Head of the Archives, Section Y, Main Group B, OKW/Chi (DF 187-A, p. 11).

DF 187-F

5. What, in general, did OKW/Chi have to do with the Abwehr?

Chi at the time of its founding belonged as a section to the then Abwehr. This subordination, however, was always leading to conflicts arising from internal conditions; the personnel of Chi was ostensibly carried in the budget of Abwehr while the majority of the intercept operators belonged to the Signal Corps and the equipment was provided by the Army Signal Inspectorate (Inspektion der Nachrichtentruppen). However, in the small army of 100,000,[29] where the officers of the Ministry of Defense were well acquainted with each other, such conflicts were always quickly resolved as differences of opinion. The critical point was that the Abwehr declared that Chi as an intelligence procurement office was a component of the competent intelligence organization, Abwehr, while the Army Signal Inspectorate insisted that Chi not only decrypted but also gathered other fundamental material dealing with communications technique which did not interest the Abwehr at all; furthermore the Army Signal Inspectorate provided the operator personnel, the equipment, the grounds and the buildings. In this permanent conflict, which did not interfere essentially with the work, there became involved T 3, i. e., the Third (Intelligence) Branch of the Troop Office (3. Abteilung des Truppenamts), as well as later the Branch Foreign Armies (Fremde Heere). Thereupon Chi belonged for a few weeks to T 3, because ostensibly only T 3 had any real claim to the decrypted messages of Chi. (That was about the beginning of the 30's). However, the Abwehr established the fact that the trips abroad by Chi, e. g., to Budapest[30] and Vienna,[31] were paid for by it. This claim was more convincing and thereupon Chi returned as a section to the Abwehr. At the same time Chi was

---

29. The strength allowed by the Treaty of Versailles.

30. For OKW/Chi's relations with the Hungarian cryptologic organization see FENNER's account in DF 187-D, pp. 1-3.

31. For OKW/Chi's relations with the Austrian cryptologic organization see FENNER's account in DF 187-E.

DF 187-F

still responsible to the Army Signal Inspectorate, merely that this latter was not concerned with decrypted diplomatic messages. However, everything else had to be presented to the Army Signal Inspectorate. When, after the founding of the Forschungsamt, it could be seen that GOERING intended to inject himself into the secret intelligence service of the Wehrmacht, General FELLGIEBEL was already entertaining the idea of freeing Chi completely of its dependence on the Abwehr. On the other hand, the interest of the Abwehr in the decrypted messages of Chi had increased materially. In the discussions which took place the Abwehr won and Chi remained with the Abwehr as Group IV, but in respect to personnel and pay it was subordinated to the Army Signal Inspectorate. When CANARIS became Chief of the Abwehr in 1935 relations became more strained. Rumors were already appearing regarding the creation of a Reichsabwehrorganisation from which General FELLGIEBEL as Inspector General of Signal Troops expected and feared merely a strong Party influence on the secret intelligence service. Since at that time GOERING's authority was very great, there was actually danger that in such a case the decryptment of messages of foreign governments would be taken away from Chi and that one day the Wehrmacht would be without this information and that Chi would have to go into a new war inadequately trained due to lack of practice material. Therefore FELLGIEBEL desired to get Chi out of the "political channel" as in his conversations with me he called this threatening danger. He made use of one of the next conflicts to force the substitution of a single subordination in place of the troublesome double subordination of Chi and this time he won his point and about the middle of the 30's Chi was finally removed from the structure of the Abwehr and subordinated to the Army Signal Inspectorate and its successor organization. As far as official connections with the Abwehr -- these were not disturbed. The Abwehr received the decrypted messages daily and on its part turned over to Chi such information as concerned the latter. But the Abwehr could neither give orders nor take disciplinary action; and the intercourse between it and Chi followed the same service principles as, for instance, between the Attache Group and Chi. In

DF 187-F

respect to personnel, administration and discipline the Signal Corps had sole responsibility.

6. What cooperation existed between OKW and Abwehr intercept units?

I know nothing of any such relation. And I cannot conceive that it ever existed. With my close collaboration with my chiefs I must necessarily have heard at some time that such a connection existed. No connection with the Abwehr ever appeared in any plan showing distribution of assignments! Any such connection would also have run directly counter to the idea of General FELLGIEBEL; and if it had existed I should surely have heard of it from him. Moreover, Generals THIELE and GIMMLER[32] would at least have made some mention of this connection during the frequent conferences, if it had existed. After all there were only very few official secrets which remained limited to a few officers and officials within an agency, but a permanent secret of this type would necessarily have been mentioned, for the simple reason that PLANKERT[33] and GROTZ[34] would not have been able to cover up the fact that they had reported to one of the officers of the Abwehr during their visits in Berlin.

7. What cryptanalytic work was attempted by the Waffen-SS?

I did not know that the Waffen-SS (Armed Protective Guard of the National-Socialist Party) ever made any attempt at cryptanalysis. It is possible that this question is based on a misunderstanding. When the Forschungsamt was founded, its members formed a special SS-Formation; in any case they were all members of the SS and were promoted in it.

---

32. GIMMLER, Major General, Chief of Signal Equipment and Testing Branch Army Ordnance (Wa Pruef 7) 1939-1943. After FELLGIEBEL and THIELE were hanged for their participation in the attempt on HITLER's life, Major General GIMMLER succeeded them as Chief of the Armed Forces Signal Communications Group.

[illegible] the OKW/Chi intercept station at Madrid, Spain. (DF 187-A, p. 22).

34. Oberlt. GROTZ commanded the OKW/Chi intercept station at Sofia, Bulgaria. (DF 187-A, p. 22).

DF 187-F

8. What do you know about the work of agents? How was the work set up and handled, as for instance, in the Referat Vauck?[35]

I have already expressed my view on this. Please check my statements and reports.[36]

Work was done on networks of the French mainland, of the Balkans and Upper Italy, in French, English and Italian (?). Possibly still other languages appeared but I am no longer certain because I never had any original messages in my hands. The cryptographic systems, generally book ciphers, were in most cases solved only subsequently, i. e., after one had succeeded in arresting an agent who had compromising material. If the title, author and edition of the books used had become known, it was often several weeks, even in important cases, before one could procure these books. If the fortunes of war were favorable and the nets continued in existence in spite

---

35. Referat Vauck was a German cryptanalytic section working under a certain VAUCK on the solution of foreign agent traffic. Until mid-1944 this section was subordinated to the German Army cryptologic organization (OKH/In 7/VI) but in 1944 it was transferred to OKW/Chi. VAUCK, who was never located by TICOM for interrogation, is described by FENNER as 1.75 meters tall, broad-shouldered, fat, fair, blue-eyes, round head, divorced, with two children, honest and fair-minded.

36. See the oral interrogation of FENNER, TICOM/I-200, par. 37: "VAUCK never had to deal with any American agents' systems, but British agents sometimes came up in the Balkans in connection with MIHAILOVIC. He never saw this section at work, and does not know what these messages looked like. He know that there was never sufficient material to break the keys, and they were only read after the agents had been captured; he believed that traffic was occasionally read currently after the key had been compromised by one of the agents without the knowledge of others. He was unable to give any names of specific examples. In the West, all British agent traffic was in French language, and he thought that they were normally Frenchmen based in London. All those captured were French, and they never took any British or Americans. Two or three times, they were able to play these French agents back after they had been captured. He thought the system employed was some kind of book cipher with subtractor; TRAME would be able to give more details. Also Dr. KEINER worked under VAUCK, and might now be in Berlin, where before the war he had been employed in the [illegible]. He said that no special secrecy was attached to [illegible] inside the organization.

At the end, VAUCK had about 12 men, originally he had had more; when OKH heard that he was to be transferred to OKW, they took the opportunity of stealing several of his people. VAUCK was a very nice, honest man, and was not a Nazi."

of the arrest, this circumstance was utilized to stage deceptive traffic, to institute so-called "agent games". In such cases one succeeded in having arms and edibles, for instance, dropped at prearranged points or in getting further information through the continued traffic. As a rule, however, the subsequently decrypted messages only brought confirmation of what was already known. And it is only in this that I see any results from the work. Frequently the agents called attention to the fact that people of their group had been arrested and that a change of key must be made. Once it happened that French agents made merry over the fact that the Germans had come to block off a spot appointed for a parachute drop but did not have enough patience to wait and drove away before the machines arriving from England had dropped their load. There may have been some 50 messages decrypted weekly, among them some, to be sure, which were almost a year old and hence had only historical significance. Since the arrest of the agents was not a function of the Wehrmacht and consequently the entire handling of the business was not concentrated in the hands of one person, the reporting route was complicated and time was often lost uselessly even though the opportunity for picking up the different agents was favorable. According to my experience it is a mistake if the decrypting agency and the executive powers are in different hands. Naturally there are different organs, for no one would think of assigning police duties to his cryptanalysts, but the German mistake was that the Wehrmacht gathered all necessary information but then had to turn over the executive action and let the SD wind up the affair. Precisely in this connection the constant tension between "Field Gray" and "Brown" or "Black" had especially harmful consequences.

I can give absolutely no details regarding the constitution of the solved cryptographic systems. I received the completely decrypted messages for my information, for the most part they were already old and therefore without much current interest. In order not to lose time, VAUCK reported immediately and independently to the executive unit as soon as a decryption was made, while the offices of the Wehrmacht which might be involved merely received the decrypted messages for their information.

DF 187-F

9. What was your opinion of the papers circulated by SCHAUFFLER in the Auswaertige Amt? Did you ever contribute to these papers?[37]

Since Dr. SCHAUFFLER was considered an analyst, I assume that the "Technical Reports" ("Technische Berichte") contained the description of the course of solution of some complicated cryptographic system. I think I recall that the Foreign Office did not prepare regular reports but only issued one from time to time when a system had been solved. Possibly some such report is involved in the question. I never got to see one of these technical reports.

Since SCHAUFFLER was an experienced cryptologist and a shrewd person, I assume that his reports were sensible and contained only what was essential. I never wrote anything for the Foreign Office. This does not exclude the possibility that some one of my reports or drafts was handed over by my Chief to the Foreign Office (Cryptologic Bureau) for them to read without my being informed of the fact. In that case, however, such papers would not have been issued under my name but quite certainly over the signature of one of my superiors.

10. What can you tell about German General Staff Intelligence Studies on Russia? What agencies existed for the gathering of material for the intelligence studies, who composed the personnel, and what was the product of their work? Were publications of such agencies distributed generally to cryptographic or cryptanalytic units?

A few times there "passed over" my desk, i. e., were routed to me for information, maps with entries on the occurrence of raw materials such as iron, copper, etc.; hemp, flax and other raw material of the textile industry; areas with surplus grain and areas with grain shortages, and dozens of other materials of economic importance from the USSR. With these there were statistics, diagrams and accompanying text. The pamphlets were about 30 cm x 40 cm in size; their classification was TOP SECRET (geheime Kommando-sache). I never paid any attention to the agency preparing them. I do not know what person provided the data or who worked them up. In conversation with

37. For examples of the type of papers meant see TICOM/D-3 and D-33 in which are collected translations of the technical papers written by members of the Foreign Office Cryptologic Bureau and circulated within the Bureau.

DF 187-F

a colleague we assumed that the HAUSHOFER's, father and son, were concerned in the work. So far as I know, both later fell into disfavor with HITLER. No published information was known to me. Since I am not an economist, my judgment is that of a layman, but I did get the impression that these studies had been prepared with care and with an excellent professional background.

11. What do you know about the Russian signal intelligence organization? Did the Germans have any contact with the Russians, White or Red?

No. I am not acquainted with that field. Again I would refer to the former Russian officer SACHAROW interned in Haus Alaska[38] who is surely well informed on this point because he was an expert.

12. What was published by the Germans concerning Russian order of battle? By whom was it published and when? Are there any copies to be found?

I cannot answer this question because the matter is entirely beyond my knowledge.

13. Did OKW/Chi keep a list of terms of Russian mechanized equipment, guns, planes, etc.?

No such compilation is known to me because that field lay outside my range of activity. I assume there is an error here: probably the Army Cryptologic Agency (OKH/In 7/VI) did compile such lists and possibly the Ordnance Office (Waffenamt) as well.

14. Are any atlases and maps of Russia available? What sort were available and by whom were they prepared?

The problem of procuring maps of Soviet Russia is difficult. The captured material was re-worked in Berlin in a cartographic office of OKW since reproductions, with place names in Latin script, were required. I know that even in 1944 the collection was still far from complete and that maps of all types were gladly accepted. Once Chi received some captured maps from the

38. During his period of int... in Europe FENNER was interned at the European Command Intelligence Center (ECIC) at Haus Alaska, a private residence at the Center reserved for important persons under interrogation. SACHAROW was interned there at this time and was being interrogated by the Director of Intelligence, European Command. No interrogation of SACHAROW was made by the TICOM representative.

DF 187-F

Cryptologic Bureau Helsingfors (Mikkeli)[39] which were taken at once to the above-mentioned office. They had merely been loaned by Mikkeli and the reproduction had to be carried out quickly. These were maps of eastern Karelia. The Russians had old maps from the Czarist period in the ratio 1: 42,000; 1: 84,000; and 1: 168,000 and new maps in the ratio 1: 25,000; 1: 50,000; 1: 100,000 as the most important General Staff map, also in the ratio 1: 2,500,000 and 1: 5,000,000. Only the western border areas and some sections of east Asia were based on new measurements while the other metric maps were merely recomputed from the old measurements. So far as I know all maps were based on military surveys since only maps of insignificant areas were made for civilian use. I can give no information as to the value of the maps. They were printed in four colors, sometimes in more. The old maps from the Czarist period were black lithographs and of no value to artillery men. The new maps are said to have been more exact, particularly the newly surveyed western areas. East Asia was surveyed in large part from the air. Who prepared and drew the German (originally Russian) reproductions I do not know. I have forgotten the official title of the cartographic office but it can be found in telephone directories of OKW. The office with which I had to do once was in Lustzowstrasse. All the new Russian maps were recomputed on Krueger-Gauss coordinates with Greenwich as 0°. For daily use Chi preferred the atlases of Stieler, Velhagen und Klasing, and Ullstein: otherwise the official maps which were available and which the other groups of Chi required for their work (cable lines, high-power transmitters, intercept areas, etc.), were used.

15. What was the procedure with German patents on communications equipment? Were there any "secret" lists of such patents? Where would they be now?

Patents were issued by the German Patent [illegible] when the legal patent requirements had been fulfilled. Whether they had been fulfilled was determined by the competent examiner of the Patent Office. Any

39. The Finnish Cryptologic Bureau which had been located at Helsingfors (Helsinki) was shifted during World War II to Mikkeli.

DF 187-F

New York foreign patent lawyer can give you full information regarding the procedure. If it was in the interest of the national defense or of the security of the country that a patent, hence also the letter patent, should not be turned over to the public, then a secret patent was granted upon application for a secret patent and an examination of the application. The only characteristic of a secret patent was that the letter patent was not made public. According to patent law all other letters patent can be examined in the German Patent Office. Letters patent for secret patents could only be seen by a person who had received permission from the German Patent Office. Such permission or approval was granted to but a few people, naturally upon application. It is a matter of course that national defense was given special consideration in this connection. Thus the Cipher Machine Company Enigma had secret patents; so too, of course, did Siemens and other big companies which had armament contracts. Special lists were kept of secret patents. Then if a representative of the agency, let us say Oberinspektor MENZER, came to the competent official of the German Patent Office, a list of the most recent secret patents was shown him. The idea that possession of the patent document is identical with the possession of the necessary knowledge is obviously erroneous. In Germany it is the idea that is patented. The realization of that idea is shown to be possible, to be sure, but the road from the protected patent claim to the completed construction is long and full of surprises. If cipher devices of any kind were to be patented by OKW, then the paper work was performed in the Ordnance Office (Waffenamt). The Ordnance Office filed the patent claim; it also paid from public funds the examiners' fees and the patent fees until the patent expired after 25 years. Of course, the Ordnance Office kept lists of the secret patents for which it had applied and which had been approved by the Patent Office. What became of ..

16. Do you recall any leads or ideas of American, British, or other nationality patents which were important to the work of OKW/Chi?

I do not know any American or English patents in the field of cipher machines. When Chi was negotiating with Siemens in the 20's for the construction

DF 187-F

of their cipher machines, the American HEBERN was mentioned among foreign inventors. Chi had a prospectus of his machine but the description was naturally in such general terms that there was no information regarding the method of encipherment itself. OKW/Chi never did find out whether any machines of the Hebern-Electric type were actually built. I do not know that American or English patents were ever useful for the work of Chi or furthered the development of German ideas by providing valuable information. However, my judgment may only be subjectively correct because I do not know the foreign cryptographic patent objectively enough to have a right to venture an opinion.

17. Do you know the names of any American, British or Russian cryptologists?

I do not know the name of a single American, English or Russian cryptanalyst.

On the basis of the book by YARDLEY[40] it was revealed that America did cryptanalytic work during the First World War with very good results. Nothing was more natural than to assume that America would also use this exact means of obtaining intelligence in this war. During the war an American newspaper published a short article on some USA organization which was fixing the nationality and location of unknown foreign transmitters in an exceedingly short time. Now since such recognition is not always possible unless the radiogram is decrypted, Chi concluded from this that America must have a cryptanalytic unit on a broad foundation. But, even if this report should have been exaggerated, it must be assumed at least that people were busying themselves with this problem in the USA. There was nothing to justify the assumption that this organization would have to be an insignificant one! Later there came from Africa the entirely credible, although unconfirmed, report that the USA was maintaining a cryptanalytic service there using Hollerith machines. At OKW/Chi it was therefore considered a fact that

40. YARDLEY, Herbert Osborne, "The American Black Chamber", Indianapolis and London: the Bobbs-Merrill Co., 1931. Reprinted, New York, 1933, London, 1934. History and work of the Cryptographic Bureau, officially known as Section No. 8 of the Military Intelligence Division (MI-8).

DF 187-F

cryptanalytic work was being done in America. After the landing in France in connection with some operation or other a secret report of the American Signal Corps fell into German hands. In this report there was also something on the question of cryptanalysis. In that connection I got the impression that in American military circles, just as in German circles, the question was occasionally raised whether the whole cryptanalytic effort made any sense whatsoever! I knew from my own experience these questions which allow one to infer a priori that the questioner considers every decrypted message a successful fraud which the enemy has thought up cunningly; less intelligent people even go so far as to ask: "Why don't you decrypt only the important messages?" In any event the American critic came to the laconic decision: "Either the decrypted message contains the truth or no truth at all!" Such a saying could only be coined by a man who not only has a thorough technical knowledge of cryptanalysis but has had a chance to convince himself frequently of the connection between the decrypted message and the truth. Consequently there was absolutely no more room for doubt as to the existence of an American cryptanalytic service under purposeful leadership. I never heard about the English cryptanalytic unit. Chi assumed as a matter of course that, due to the success of Sir Alfred Ewing in World War I, the cryptanalytic service would be in capable hands this time, too.[41] When during this war England endeavored to recommend to the Turkish Government the use of an English cryptographic system at Ankara, this did not remain concealed from Chi, and the only

41. A reference to the speech delivered 13 December 1927 to the members of the Edinburgh Philosophical Institution by Sir Alfred Ewing, Principal of Edinburgh University, a complete report of which was issued with Lord Balfour's tribute to Sir Alfred Ewing in the Edinburgh newspaper, The Scotsman of 14 December 1927. In the speech Sir Alfred Ewing gave an account of the secret service work in which he was engaged during the war. Though the main features of the work had been disclosed before (for example, in Mr. Winston Churchill's The World Crisis and in the Memories of Lord Fisher, Admiral of the Fleet) Sir Alfred Ewing recounted for the first time many details in connection with the British World War I cryptanalytic unit of which he was the head. This branch of the Admiralty service, called "Room 40", also received much attention in the life of Sir Alfred Ewing written by his son under the title: "The Man of Room 40 - The Life of Sir Alfred Ewing" by A. W. Ewing, Hutchinson and Co., (Publishers) Ltd.

possible deduction to be drawn was that England was again active in this field and was reading the Turkish systems at least. But if England was working successfully on Turkey, then there was nothing in the way of its working on other countries since some of the French diplomatic systems were certainly no more difficult than the Turkish. There was an unconfirmed report after the First World War to the effect that some former Russian naval officers who had worked during the war on messages of the German Baltic Fleet were engaged in the cryptologic work of the Kremlin at Moscow. From the development of the Russian Government cryptographic systems from types which could still be solved down to the digit codes with groups of different lengths and with one-time additive pad which cannot be solved with even the most modern means, the inference must be drawn that there are in Moscow at least a few men who investigate their own cryptographic systems, ascertain the weaknesses and regularly provide for replacement whenever a system begins to compromise itself due to over-extensive use. Reports on the strict selection of personnel in the Fourth Section of the Russian General Staff also suggest at the same time that there, too, the question of the security of cryptographic systems is given increased importance. However, the purely analytic knowledge of the cryptographer cannot be separated from the knowledge of the cryptanalyst. In reality it is the latter who, according to my experience, fructifies the cryptography of his own country. I have never seen things go the other way. For this reason it was assumed with a probability bordering on certainty that Moscow has a cryptanalytic service.

In captured Russian cryptographic instructions of the army there was found such a clear expression of ideas, such an exact differentiation between "digit" (Ziffer) and "number" (Zahl) that what was to be found there was no thoughtless piling up of words but rather a classic clarification of words by people who must certainly have occupied themselves with cryptanalysis. The similarity between diplomatic systems and those of the highest staffs also let it be recognized that the ideas all came from under the same hat and Chi

therefore regarded as proven that there was a single central cryptologic agency in Moscow.

18. Do you know of any cryptographic organization of a public character in Europe? If so, what were the names and locations of such societies? Do you know the names of any members?

Shortly before the outbreak of the war one of my cryptanalysts brought me a little announcement taken from a French journal which advertised a course in cryptanalysis. I believe the price was 20 francs. Regarding this information some remarks were made concerning the naivete of the people and the suspicion that possibly the French General Staff was behind it. But no attempt was made to follow up the matter and it goes without saying that we did not write to this organization because our security rules forbade it. Certainly Chi did not expect any success from a camouflaged inquiry. The seat of the organization was Paris, if I remember rightly. I do not know the name.

19. Give an account of your liaison with the Japanese nationals NISHI and SAKURAI.[42]

---

42. This question was put to FENNER in written form because of a doubt which arose in the minds of the interrogators at his oral interrogation concerning the relations of OKW/Chi and the Japanese. At the first interrogation of FENNER (17 Sep 1946), he admitted having known HAYASHI, who had come to Berlin at the beginning of the war and had given the Germans the originals of the Brown and Gray Codes; FENNER claimed, however, that he did not know how they had obtained these books, and he said nothing was exchanged between OKW/Chi and Tokyo though this might have been done between OKH and Tokyo. At the third interrogation of FENNER (19 Sep 1946) FENNER was asked whether he knew the Japanese NISHI and SAKURAI. At that time FENNER replied that he knew both of them vaguely, but had little contact with them. NISHI had been at Budapest with HAYASHI: SAKURAI remained in Berlin, but FENNER claimed to have seen him only three times. FENNER was then informed by the interrogators that KETTLER had stated, FENNER had passed American and other material to these two men. According to the report of interrogation: "FENNER was very startled, and said that he had helped them with Russian and American traffic, mainly by giving them raw material. Further questions elicited that he had also given them copies of the VNs, mainly American and French decodes. KETTLER had ordered him to give them everything they asked for. It was pointed out to him that this hardly conformed with his previous statement that the liaison was very weak. He said that he had meant "spiritually" (geistig) , not "practically" weak. Both prisoner and interrogators remained unimpressed by this argument, and FENNER was told to give a written account of the whole episode." (Excerpted from TICOM/I-201, paragraphs 1 and 29). FENNER's answer here coincides substantially with the description of the relations of OKW/Chi and Japan, as given by him in DF 187-D, pp. 9-10.

DF 187-F

I never worked with the Japanese NISHI or with SAKURAI or with any Japanese at all.

I have already stated at my interrogation that HAYASHI arrived in Berlin shortly after the outbreak of the war and brought Chi the American Brown and Gray codes. Later on HAYASHI sometimes made statements regarding Soviet Army systems which had supposedly turned up in the Far East. These reports were noted and thereupon regarded as settled because they had no practical value, either because the information was not pertinent or because the observations, although correct, did not apply to the German Eastern Front. Chi and HAYASHI were at that time less interested in any particular system than in proving or checking the assumption that Army systems which had been replaced at the Soviet West Front might turn up at the East Front in Asia. All the information HAYASHI was able to get from Tokyo in this respect was so sketchy that it was not possible to prove that systems which had been replaced on the West Front ever did turn up in East Asia. Chi was never able to get a systematic account of the cryptographic systems used by the Soviet Army in East Asia.

Already at an interrogation I stated that the relations between Chi and the Japanese were of a superficial nature. This is not changed at all by the fact that the Japanese received material from Chi. The relation remained superficial because there could be no collaboration between Chi and Tokyo. I have already pointed out that HAYASHI was practically cut off from Tokyo, that there could be no thought of regular courier connections and that there was no regular interchange of telegrams between HAYASHI and his home office. So, if I was occasionally called in when HAYASHI was calling on my Chief, we talked in a friendly way about all possible things except cryptanalysis. In 1944 HAYASHI again paid a call on Colonel KETTLER. This time I was called in, probably because KETTLER wished to hear my opinion. HAYASHI said he was no longer getting any information of any practical use and he therefore asked that we let him have VNs for his information. It was clear to us that such information would naturally get to the Military Attache and

DF 187-F

the Ambassador himself. Therefore it was impossible for us to promise HAYASHI anything on our own responsibility. However, KETTLER put that up to his Chief,[43] who supposedly discussed it with JODL[44] and, on the basis of a basic order that the Japanese were to be given anything they wished, I was informed that VNs might be given the Japanese to a limited extent. It was agreed with HAYASHI that he was to have these VNs picked up once a week at my office, but only after calling on the phone so as to avoid coming to no purpose. This happened and at intervals of a week, later only every two weeks, NISHI or SAKURAI received some VNs in my front office or from me personally. These VNs were not limited to those dealing with America or any other country but whatever might be of value was turned over as we saw fit. The first four or five batches were selected by my section heads for the different countries. That did not work because I did not get the messages on time, inasmuch as they had to be gone through and recorded; for instance no VNs were to be turned over which might be damaging to German interests in any way. In short, to unify things I instructed Dr. SCHAEDEL of the Archives to pick out suitable VNs. And this was done with the necessary tact. In approximately five months the Japanese in Berlin received at most 10 such selections. Each batch contained less than 20 VNs. In February there were no deliveries to the Japanese, the excuse being the air attacks. It was also due to the ever more evident development of the military-political situation which would in any event have led to an interruption of our relations with Japan. When HAYASHI became Military Attache in Budapest he asked, curiously enough, for the occasional sending of English telegrams in plain code. Ostensibly he wanted to work on this traffic along with several gentlemen.

---

43. At that time presumably Generalmajor GIMMLER, Chief of the Armed Forces Signal Communications Group, or Generalmajor FRAUN, Chief of the Signal Communications Affairs.

44. Generaloberst JODL, Chief of the Armed Forces Operations Staff.

DF 187-F

Three or four times HAYASHI received some "practice messages"; then the delivery of such material ceased because in view of the now difficult communication it was only a useless bother, even though only a few telegrams were involved. HAYASHI received this material through the Chief of the Hungarian cryptanalytic unit.[45]

NISHI was ostensibly an assistant to the Military Attache. Late in 1944 or early in 1945 he became Lieutenant Colonel. What his functions were I do not know. I do not know the rank of SAKURAI nor do I know what duties he was supposed to perform. I once talked with the Military Attache himself: it was one forenoon in 1945. We drank cognac on an empty stomach and said not a word about military affairs. I did not become acquainted with other Japanese.

20. What use did cryptanalysts make of OKW/Chi library and archives? How were reference materials such as news broadcasts made available to cryptanalysts? What were the reference materials available? Where are they now?[46]

Every practical cryptanalyst knows how frequently he encounters place or family names of which he has been able to interpret only a part. Every practical cryptanalyst knows how often in partially solved telegrams current events are mentioned for which he does not know the precise political terms. Every practical cryptanalyst also knows how important it is if he can ascertain quickly what important thing has happened on that day, not only at home but throughout the whole world which may tie in with the name he has interpreted and the time he has fixed. And suppose an event lies many months back; one cannot expect the cryptanalyst to burden his memory with a lot of ballast which is quite unnecessary for him. One need only to imagine how agreeable it is for the analyst if he has a readily accessible central unit

---

45. General Istvan von PETRIKOVITS. For the relations of OKW/Chi and the Hungarian cryptanalytic unit see DF 187-D, pp. 1-3.

46. For an excellent discussion of the Archives of OKW/Chi and their importance see the translation of a lecture on the OKW/Chi archives delivered in March 1945. "The Significance of the Archive as Aid to Cryptanalysis and a Source of Information". (DF 204).

DF 187-F

which gives him all conceivable information. The information service of the Archives was an institution which was used day in and day out. As far as I can recall, the Archives got seven questions in the first week, some 70 in the second week; no further count was kept because the idea had taken hold and was fully appreciated by all the cryptanalysts.

The actual secret Archive of Chi was probably burned in Werfen. Part of the file of decrypted messages (VM-Archive) was completely burned at the time of the air attack on 24 November 1943; those were the messages of the years 1940 to August/September 1943. Older messages, down to about 1937 were located with the Chief of the Army Archives in Potsdam and in part in the document room of the Ministry on the Landwehrkanal, in the building at Tirpitzufer 38/42. What became of these documents I do not know.

21. Did OKW/Chi keep a list of abbreviations, of terms of standard translation or special phrases? Where is this material now?

For years OKW/Chi kept alphabetic lists of foreign abbreviations and their meanings written out in the foreign language and with German equivalents. I think these lists were compiled in Group I.[47] These lists were supplied to me[48] but were practically unnecessary because none of the cryptanalysts made use of them. The few abbreviations appearing in encrypted messages were known or were soon interpreted. Those working on press and propaganda transmissions may have needed these abbreviations, but I am not sure.[49] I never saw translations of special phrases. There were lists of English, American, French, Russian and Italian abbreviations. I burned in Berlin the lists charged to me; the other groups probably did that in Werfen.

---

47. FENNER refers here presumably to the pre-1944 organization of OKW/Chi, in which Chi consisted of four Groups: I, II, III, IV. Group I under Major ANDRAE was charged with the employment of technical and personnel resources [illegible] (see DF 187-A, p. 21).

48. FENNER was chief of Group IV: charged with the decryptment of foreign cryptograms.

49. Group III under Major KAEHLER was charged with the interception of foreign press and propaganda.

DF 187-F

22. What dictionaries were used by OKW/Chi? Are any now available? Describe the work done by Sdf. KUEHN on military dictionaries.

Chi used the dictionaries ordinarily used in Central Europe. These were published by Toussaint-Langenscheidt, Schmidt, Sachs-Villatte, Pawlowski and others whose names I do not know. Most of the dictionaries were the private property of the cryptanalysts. The firm Harrassowitz in Leipzig could give the best information on dictionaries including those in oriental languages. However, all these dictionaries had the disadvantage that the newly created words of diplomatic policy could not be contained in them. These concepts and the corresponding terms the cryptanalysts had to memorize in their practical work. But no collection of these new words was compiled. KUEHN did not come to my unit until the end of 1944. The reason was as follows. The need for military dictionaries was, of course, great. For the development of the military language is much more stormy than that of scholars and diplomats. Not merely does military technique leave its imprint but even the jargon of the soldiers affects it. Everybody who translated and everybody who came into direct contact with the enemy linguistically needed dictionaries. The result was that dictionaries were compiled in various offices. Industry and zeal may have been displayed in the process but there was not always the requisite special knowledge which is indispensable if something is to be created that will be good even a decade later. In order to avoid waste, to produce something unified and not to use up needlessly paper which was already in very short supply, Chi asked KEITEL to issue an order according to which the preparation of all military dictionaries would be turned over to me. After all, the best trained philologists were working under me and nowhere else was there such a logical place to collect the entire vocabulary required and to provide illustrations of use such -- [illegible] dictionary. The suggestion was approved and I took over KUEHN with the few people he had. Late in 1944 and early in 1945 the compilation of the English military dictionary with consideration of "slang" as a part of the scheduled work was drawing to an end. The proof sheets were already being gone over. A Russian military

DF 187-F

dictionary was in the preliminary stages. The material was burned at Werfen. Possibly KUEHN saved some private material. I expected a great deal of this work myself because the extent of the work, the exactitude of the collection, and the arrangement of the books, would certainly have met with approval abroad after the war.

23. Do you feel that information produced by the cryptanalytic people was properly handled? Who evaluated the information? How and to whom was it disseminated? What did the recipients do with it?

I had the impression and gradually became convinced that the secret Archive (Information Section) evaluated the VNs carefully and according to correct principles; otherwise requests would not have come in from outside agencies. I know, for example, that the General Staff once wanted to find out quickly whether anything was known from the VNs or other sources regarding Soviet Russian preparations for war. While previously the answer to such a question was incomplete and took three days, the complete, finished answer could now be given in three hours. The Archive gave only objective information without any interpretation or criticism. At a time when propaganda is endeavoring to dim the eyes of even the shrewdest people to reality, the mere existence of such an information unit based upon documents would have proven its worth in a very short time. As long as this Archive was still under my control, it was my ambition and that of my associates to create an institution which would tell the truth and would therefore enjoy complete confidence. The time for creating such an organization had meanwhile become ripe.

The distribution plan for the VNs is not known to me. Consequently my knowledge in this regard is extremely sketchy. Lieutenant Colonel von KALCKSTEIN[50] or Dr. SCHAEDEL[51] could best give information.

---

50. See DF 187-A, p. 11 where Oberstlt. W[illegible]KSTEIN is entered as the Chief of Section X. [illegible] and Telegrams. Day Book) Main Group B. For FENNER's characterization of von KALCKSTEIN, see DF 187-E, p. 18.

51. See DF 187-A, p. 11, where Dr. Herbert SCHAEDEL is entered as head of Section Y. (Carding items from decrypted messages and from plain-text messages, distribution of secret information) Main Group B. Dr. SCHAEDEL had been instructor at the University of Leipzig. For FENNER's characterization of SCHAEDEL see DF 187-E, p. 24.

DF 187-F

My office was merely told how many copies of the VNs were to be made. Distribution of the VNs and control of them was not in my hands, neither was the picking out of specific VNs which were required for any particular purpose.

Cryptanalytic reports, as I have already stated, were originally written once a month, then perhaps from 1927 on only every three months. There were about five copies in all. From 1933 on, only annual reports were prepared, generally in two copies, in a few exceptional cases in three copies.

24. Describe the preparation, selection of material, publication, translation, and distribution of the VNs.

Preparation: The entire traffic was sorted in the Telegram Registry,[52] separated according to countries, and delivered as quickly as possible to the head of the pertinent language section or his representative. There the material was divided according to four points of view: messages currently able to be decrypted; messages worked on but not yet able to be decrypted; unknown, i. e., those cryptographic systems not yet analyzed; and rejects, insofar as these had not been eliminated in the Registry.

Messages currently able to be decrypted were freed of their reencipherment or immediately decrypted, and the messages not yet "ripe for VNs" were placed in the hands of an expert. Unknown systems went into a special collection and were "observed" as we said at Chi, i. e., watched for similarity of type, the frequency of the messages sent, in short all criteria which we desired to have cleared up before engaging in systematic work on a system. I have already said elsewhere that good philologists decoded telegrams using the solved codes. In so doing newly obtained interpretations were naturally filled in, even in those codes which were in an advanced stage of solution. I saw to it that even a clever man did not have to work on more than two plain codes unless solution had already progressed so far [illegible] but only decoding was involved. Once the telegrams had been stripped of encipherment and decoded, one began the

52. According to the OKW/Chi organizational chart of 1944, the Telegram Registry was under Group a of Main Group B. (DF 187-A, p. 5).

DF 187-F

Selection: The practiced cryptanalyst sees very quickly whether a telegram contains political or military-political information or merely administrative matters which are of no special importance. So-called passport messages are quickly recognized, as are also the reproduction of voices of the press. Of these messages only relatively few could claim any objective interest. Moreover I had observed that nothing is so likely to minimize the value of the VNs in the eyes of those who receive them and do not realize how much effort it costs to produce them as to include every unimportant matter! Therefore in selecting the VNs to be produced we considered as important: the daily situation reports of the Ambassadors and Ministers; comments of the press, because from these the specific attitude of the foreign countries toward certain problems could be seen; and finally actually new reports and instructions from the central authority to its Ambassadors, Ministers Plenipotentiary, and Ministers (and vice versa). According to my observations over many years there was generally seven times as much decrypted as was issued in the form of a VN! It is true, I occasionally got instructions that special importance attached to certain messages but such instructions always coincided with the opinions of myself and my colleagues. I gave my co-workers as free a hand as possible in the selection. I could do this without feeling concerned for it is the natural ambition of the cryptanalyst to offer as objectively interesting information as possible, even though messages which were only subjectively interesting contributed to the silent satisfaction of the workers, e. g., the description of a supper at which certain gentlemen handled knife and fork in a not exactly skillful manner. The many passport and economic messages were of no interest higher up but if they were included occasionally, likewise even less important messages, that was usually due to the fact that the analyst on the basis of his knowledge attributed greater importance to such messages than his superior, for instance, who was primarily interested in the press. The question of what was really important was never correctly answered and can never be answered in a completely satisfactory way, because a message which was quite unimportant today may be very important two years hence! I and my colleagues took the point of view, therefore, that it was better to bring too many

unimportant messages than to have failed to bring some important ones on VNs: "Let the gentlemen at the top separate the chaff from the wheat!"

In the case of Army radiograms there could be no rule of thumb in evaluation. A seemingly insignificant message in which a new military unit is named can under some circumstances be more important than a decrypted order to attack which is already known from some other source. For this reason the decrypted radiograms of foreign armies were never included in the daily edition of the VNs; decrypted Army radiograms were also called VNs but they went into other hands where each individual message called for a careful going over. This work is a special field, with the interpretation of call signs, the attempt to show any existing periodicity in the use of call signs and wave lengths, with the preliminary evaluation, the various card files, the actual message evaluation and the final evaluation which is crystallized in a uniform report which in turn has nothing to do with the necessary putting of these secrets to good use.

Translation: Great stress was put on good translation. It was necessary to translate because with the multitude of languages worked on it was inconceivable that the officers charged with further processing would know all these languages well enough to understand correctly a decrypted message where the grammar often departed from accepted rules. In each section there was at least one cryptanalyst who knew German and the foreign language so well that in cases of doubt the German text could be brought to him for checking and for a decision. Naturally it was required that such differences as:

gewisslich	certainement
sicherlich	surement
nur	plus de, seulement
bloss	pas autrement, simple
anscheinend	probable
scheinbar	apparent

be correctly rendered, likewise the designations of offices and officials. Anything which might perhaps be false in the translation had to be indicated as questionable, originally by a question mark in parenthesis after the dubious

DF 187-5

word, later on the passage which might be inexact was underscored with a broken line. Nevertheless it probably happened that in view of the number of new technical expressions which were always coming up, one or another was not correctly rendered. The decisive factor was therefore the correct sense of the VN; and consequently any attempt to complete an incomplete message on one's own responsibility was strictly taboo. For the same reason it was forbidden to weave personal remarks into a VN: the VN must approach as far as possible the objective communication. Otherwise it would have ceased to be a Verlaessliche Nachricht, i. e., a piece of reliable intelligence. Hence if a message appeared important enough to be issued as a VN and if it had been translated into German, then it was written as a VN.

Distribution: Each VN carried in the heading the designation Chi and VN, also a notation whether the decrypted message had been sent by radio or cable. Then followed a definite statement of nationality, because the language alone was not sufficient since Egypt, for instance, used a French code. Furthermore each VN had to contain data which stamped it as an indisputable document: telegram date and, if present, the journal number of the telegram. Otherwise in case of the publication of historical commentaries or sources by the opponent the assertion could have been made that the VN was not genuine! Finally each VN had in the lower left corner a brief notation of distribution. E. g., "Abw 4 x ". This signified that four copies of this VN had been delivered to the Abwehr. This notation remained when Chi had long since ceased to be a part of the Abwehr and other agencies besides the Abwehr were provided with VNs. However, an exact distribution list was not to be given on the VN for obvious reasons, therefore it was decided to write in stereotype fashion "Abw...x". In this notation, therefore, only the number agrees with the facts, always providing that +1 is mentally added because each section had its own complete VN collection in order to be able to look up at any time solved telegrams or groups which had already occurred, etc. However, these copies could never show up anywhere because otherwise they would have had to be registered as TOP SECRET (geheime Kommandosache) documents and the mechanics of the office

would have become still more complicated. Finally there stood in the lower right corner (likewise on the last sheet) of a VN a brief indication of the cryptographic system used, e. g., F 21 or Am 1 or Rum 3, etc. That signified: France, cryptographic system Nr. 21, i. e., the 21st French system solved at Chi after the First World War; the first American system solved at Chi after the First World War; the third Roumanian system solved. However, it also happened that this notation was made more explicit, i. e., that the entire formulae of the system involved was written down, e. g., P4ZCüZw4 which signified: Polish 4-digit code, reenciphered by means of an additive sequence, fourth system solved. Later, however, these designations were often made only on the copy remaining in the section, hence it is not absolutely necessary that a genuine VN shall show this notation because the notation was significant only within the unit. On many VNs there stands in addition to this notation the initials of the responsible cryptanalyst and my own, which later dropped out because it was quite impossible to read and sign each individual VN. The reproduction of the VNs down to the last months of the war was by typewriter using carbons. This led to bothersome complaints since the carbon paper grew poorer during the war and the carbon copies likewise. Not until 1944 was I able to get authority to have the VNs written on waxed plates and run off in the requisite number. Once the requisite number of copies had been prepared, they were taken without loss of time to Lieutenant Colonel von KALCKSTEIN who undertook and was responsible for further processing and distribution. In his office was to be found the copy which ultimately came into the Archives. These copies came at first by the year, later by the month in loose-leaf binders and were delivered to the Chief of the Army Archives in Potsdam, Hans-von-Seeckt-Strasse 8, when it was to be assumed that Chi would no longer be interested in the back numbers. Thus there were delivered to the Chief of the Army Archives all the VNs of the first postwar period down, I should say, to the end of 1930; the remaining material which was ready for the Archives was in the main building in the Tirpitzufer and in my office where several annual files were burned. The binders were numbered serially, consequently the genuineness of such a document could be checked at any time.

DF 187-1

cryptogram lost its dominant position as the panacea for the pains of helplessness and became a means to a conscious end; the eye became more keen for the possible appearance of characteristic features, the imagination was stimulated and the confusion of cryptanalysis with the concept of a "Black Art" disappeared.

When now in the course of years my personnel had been greatly enlarged, new assignments were added and the daily administrative tasks bound me more to my desk than to the lecture room, when I myself had become more mature and had become convinced of what I ought better to have done, I decided to give a different form to the instruction. I gathered together in a special course on "General Cryptology" those younger cryptanalysts who after they had been observed for one or more years while engaged in practical work were designated by their section heads as gifted and I gave them instruction two days a week from 1500 hours to 1700 hours: in the first winter semester on substitution systems as basic systems and in the second winter semester on transposition systems as basic systems and on simple combined systems as well as the most frequent types of reencipherment. What had proven good in my earlier teaching I retained. Anything that bordered on play I touched on only briefly, without laying any weight on it. But the most important principles of psychology and logic were included because many of my pupils were university graduates and were receptive to a presentation which at least attempted to show the relation between cryptology and the other branches of science, in short to present cryptology itself as a science. With full conviction, however, I stuck to a simple, really primitive presentation of all the material because for enlivening the instruction I used the examples themselves, historical observations, pedagogic hints, and critical [illegible] information had been gained meanwhile it was worked into the material so that the pupils after two years had been familiarized with the basic principles of modern cryptanalysis. If I noticed that one of the pupils was not up to the requirements, I reserved the right to cross him off the list of participants. In this way I

DF 187.F

As to the actual distribution I can tell nothing, as I have already stated elsewhere. I did not concern myself with it and it was von KALCKSTEIN's duty to accomplish the distribution and likewise to check the copies returned. As I recall, there were some 10 copies of each VN prepared toward the last. The master sheets were burned in my office after they had been used. Before distribution of the VNs the most important passages were underscored by von KALCKSTEIN and his assistants to make possible a rapid scanning of the material. As to the value of such a measure opinions varied greatly. SCHAEDEL and I disapproved of this method of "predigestion" because it involved a risk that the VNs would be deprived of their character as especially valuable secret intelligence since the reader skimmed such prepared reports just as superficially and casually as he did all others. We both maintained that a VN should only get into the hands of people who have time enough to look at them until the reader had completely understood them. Those who want to read VNs just for sensational items have no right to get them! However, as I have said, other people were of a different opinion and underscored certain words in the VNs with colored pencil. Assuming wise and serious readers, this method may be very helpful, but only under the assumption I have just made. After I had succeeded in having the VNs multigraphed, each one was also marked with the call sign beneath the heading, in case it was a radiogram (to aid the statistical work of other groups of Chi) and was provided with a brief summary. That had to be done because hand in hand with the modernization of our reproduction went the organization of the Archives and the Information Section. Furthermore I desired by indicating the content to render the time-consuming underscoring unnecessary and also to force the cryptanalyst and [illegible]lator to pay strict attention to the sense of what was decrypted. The other data remained just as I have described here.

Publication: The publication of VNs was strictly forbidden. Every VN was marked "geheime Kommandosache" (TOP SECRET) and therefore was most carefully safeguarded. It was forbidden to speak about VNs and decryptment outside our workrooms. And within the workrooms only with people one knew, hence not

DF 187-F

with unknown officers and officials, so-called visitors, who came into the Ministry under some pretext or other. Every serious cryptanalyst knows the consequences of the publication of a VN. When after the World War Ambassador PAGE published the so-called "Zimmermann dispatches", in which Secretary of State von ZIMMERMANN tried to induce Mexico to enter the war against the USA, Chi made use of these publications to prove how important an exact decryptment is and how important it is that every cryptographic system be carefully tested before it is put into use. And PAGE's publication was worth more than a whole course of first class lectures! Once when an English correspondent got knowledge in the Foreign Office of an Italian VN which had been decrypted at Chi and published it in a Manchester newspaper, including a cryptographic error which had slipped by Chi, this Italian diplomatic cipher was replaced and so, as far as I recall, was Ambassador AMADORI who was then stationed in Riga! In general it was considered a rule that the interests of truth can only be served by the publication of all sources 25 years after a significant event at the earliest. Before that it may be very intriguing but so many decent people, who have erred not from evil intent but only from human insufficiency, become involved by such a publication that it is better to keep silent and wait. (For this reason, for instance, there is still no absolutely exact account of certain events of the First World War.) When the French Intelligence Service discovered that the French diplomatic systems were being worked on with success at Chi, this information alone was enough to cause the Quai d' Orsay to replace certain systems more speedily than had previously been the custom. Thus not only any publication but de facto any rumor constitutes a danger for the cryptanalytic unit, the purpose of which is not to satisfy someone's desire for sensation but to promote the security of the country which one serves by means which one prefers to employ when dynamite and blowtorches would attract too much attention without doing the slightest good.

25. Describe the training which should be given to a cryptanalyst. What are the basic requirements for a good cryptanalyst?

Regarding the advisability, indeed the necessity of a training program

DF 187-r

for cryptanalysts, there could be no argument on the basis of the experience I had early in the 20's (when I took charge of the cryptanalytic section). Concepts which occur frequently in cryptology had not been defined at all or not definitively. Consequently misunderstandings were found in quite meaningless conferences. A set of instructions written at that time by the then First Lieutenant BUSCHENHAGEN[53] with the collaboration of his employees[54] did describe the solution of several cryptographic systems but it made the error of always starting with the assumption that the character of the system was already known. Hence the technique of the special course of solution was perhaps correctly presented, but the question: "How do I solve an unknown system?", was touched on only fleetingly and therefore answered only inadequately. Cryptanalysis was carried on in a purely empirical manner; the guiding and consoling idea was: "Something sensible will occur to me." No one had as yet thought of the possibility of establishing some systematic order among the very varied systems already known. Particular names had been given to individual systems, it is true, but the essential connection between them was not yet recognized. In view of the conservative attitude of the old cryptanalysts and of their prejudices against every innovation, the attempt to bring order into the official vocabulary encountered difficulties. I therefore resolved to set up some practice problems which would depart from the usual scheme only in very minor details and had the satisfaction of seeing that even the most gifted cryptanalyst did not find the correct solution. This circumstance was considered sufficient proof of the inadequacy of the method hitherto

53. Oberlt. BUSCHENHAGEN was the founder and first director of the post World War I Cryptologic Bureau January 1920. He was later officer of the General Staff with various assignments; with the defection of Rou[illegible] fell into Russian captivity as General of Infantry.

54. Eleven persons are listed elsewhere by FENNER as members of Chi in 1922: Hellmuth MUELLER (for France); Nikolai ROHEN and Carl WAECHTER (for England); Emil Freiherr von REZNICEK (for Italy); Alfred FUCHS (clerk); Peter NOVOPASCHENNY, Wilhelm FENNER, Alfonso KLEIBERT, First Lt. SCHMIDT, Felix SCHERKE and Edith von BUECHLER (for Russia). (DF 187).

DF 167-F

used of trial and error supported by experience. A few other problems with easy reencipherments now awakened interest in a new direction. In little talks in a very limited circle I presented first the general characteristics of the systematic arrangement of cryptographic systems and then the methodical solution of basic systems which had long since been known, that is to say, those cryptograms which are derived from the plain text by a single operation. In the cryptanalytic reports, which in those days were still prepared monthly, I unsparingly corrected everything which did not agree with the new terminology, everything which was obscure and every deviation, no matter how slight, from a logical presentation. I weeded out all verbosity, every attempt to get around a clear presentation and to give an explanation in general terms. I called for a simple and naive description so that "even your superior can understand your cryptanalytic report". I accepted internal frictions because they proved to me that a critical spirit had taken hold. I did not expect any more as a beginning. However, I did forbid giving new employees general instructions for the solution of cryptographic systems and instead reserved to myself the right to start the new generation on the path which I had recognized as correct. So the new points of view gradually came to be accepted and in a few years were the general property of the cryptanalysts. However, there was still another disadvantage about the older cryptanalysts which was disturbing: a man may be an excellent cryptanalyst; he works for months, sometimes far over a year, on one or two current systems. If they are solved, others take their place which generally are not essentially different from the old systems, especially in the case of plain codes: the virtually identical vocabulary has merely been distributed differently! The activity of such cryptanalysts unfailingly led to a one-sidedness [illegible] them helpless as soon as a new system appeared which fell outside the framework of the familiar scheme. So about the middle of the 20's I collected the older cryptanalysts for a course of 90 days - each working day except Saturday - and taught them the systematic classification of cryptographic systems, all basic systems, systems showing a single combination, and the universally used forms of reencipherment. In contrast to the traditional presentation I started in each individual case with the general subject, in

DF 187-F

[illegible] to prevent the pupil from basing his conception on the special case. Then in my examples I gave special cases and asked for a critical statement which aimed at recognizing as quickly as possible every systematic feature contained in the system and of utilizing this knowledge skillfully, at checking how and when this systematic feature was recognized, indicating the "locus minoris resistentiae" and finally criticizing the system itself. My endeavor was at the same time to cause cryptology to rise from the sphere of a lower ("Kunde") - compare the common term "Wetterkunde" in Germany - to the higher level of a science (Wissenschaft). But precisely for this reason I had to refuse to give dead-sure recipes for the solution of this or that cryptographic system, that is, so to speak, a cookbook of cryptology! I taught the methods; the application I left to the judgment, but not to the whim, of the cryptanalysts. Although I had in my teaching the secondary purpose of giving the pupils a certain routine training, nevertheless the real main objective was to train them for research and for independent thinking and decision. Hence the following sequence of ideas and concepts was taken as a guide:

Meaning of the Instruction: Scientific Research Work

Purpose of the Instruction: Training of Cryptanalysts

Making Known the Results of Previous Investigations

Gathering of the Results of New Investigations

Comparison of the Old and New Results (Criticism)

Arrangement according to Certain Points of View (Rule, Systematic Classification)

Aids, Sequence of Steps, Statistics (Method)

Picking out Regularities (Scientific Recognition)

That the pupils within the limits set by this plan also became acquainted with specific aids, e. g., letter frequencies of foreign languages, frequencies of syllables, frequ[illegible] characteristic relations to one another, goes without saying. I also considered it appropriate to introduce mathematics into the subject matter everywhere where numbers could serve as a measure. The basic rules of combinatorial analysis (Kombinatorik) and of probability had to be mastered. However, the results of such a training, even though far from comprehensive, were unmistakable: the frequency count of a

DF 187-2

pursued the object of advancing only really capable people and not burdening anybody with mental ballast which he would not need as a statistical clerk or cryptanalytic assistant. As I have already mentioned, I did not accept any beginners in this course, but did demand expressly that every beginner destined to become a cryptanalyst should as his first job make a count of a plain code, then decode using a well solved code, then help on a code already in course of solution, and only then try his hand on the independent solution of a code. Of course there were cases where I departed from this rule. This happened when I had convinced myself of the tractability of a new appointee, of his imagination, his knowledge of current events and his linguistic knowledge. (I did not admit any applicant without subjecting him to a test. I had him give me a sample of his handwriting, asked about his favorite subject in school; put questions to him in the field with which he was least acquainted, not to worry him but in order to be able to judge from the reaction to my questions how he would meet unpleasant situations. I also inquired about his views on matters which were occupying the mind of the general public; questioned him regarding his relations to God; tested his powers of imagination and only at the end had him tell me all about his favorite subject in order to get an idea of his vocabulary and his temperament. Independently of that the applicant had to translate into German orally an editorial from some foreign paper and make a written translation from German into that foreign language which he supposedly knew best. If on the basis of my total judgment I had become convinced that the applicant was a personality with adequate knowledge, then and only then did I request that he be hired). This method of selection and of initial occupation proved satisfactory and I did not have to give it up until I was forced during the war to accept replac[illegible] personnel without examination, just as they were assigned me by the Labor Office through the Administrative Branch. Since the teaching would have been too burdensome for me alone I later had WENDLAND and RUETTENHAIN help me. The latter was also told (during the war) to give lectures from the field of higher cryptology to those cryptanalysts who were considered best, i. e., to those who seemed

DF 187-F

suitable not merely in respect to language but also as analysts; he was to talk also on the theory of groups and the solution of systems with complex reencipherment, to take up the problem of modern machines, i. e., everything which experience had shown would go beyond the normal ability of a practical cryptanalyst. The idea of instituting such a course sprang from the fact that during the war a number of exceedingly capable analysts were working for me who would return to their civil occupation after the end of the war. However, the cryptologic ideas of these men ought to be firmly anchored in Chi. Reports and long papers would have dissipated the working strength of these analysts who were mostly mathematicians at universities. Consequently I deemed the use of lectures and mutual discussion and practice problems after the manner of the university seminar to be the most suitable method. From then on a difference was likewise made between "lower cryptology" and "higher cryptology" whereby the material taught by HUETTENHAIN belonged to the higher group as I mentioned a few lines back. On the basis of my experience I can merely say that these courses in general, i. e., lower cryptology and those in higher cryptology, proved their worth. The uniformity of expression, the abundance of material offered, the selection of suitable exercises, and the constantly injected repetition of already known topics, not merely enriched the pupils' knowledge and deepened their understanding, but allowed them to ripen into men from whose mental fruits a good harvest was to be expected. Due to lack of space (one of my buildings had been completely destroyed in November 1943 by air attacks on Berlin), I had to discontinue my instruction. HUETTENHAIN was still giving lectures in the winter 44/45 until conditions in the building made even this instruction impossible.

The guiding principle of all the instruction can be summed up in the following words: "A cryptographic system is a regular deviation from the forms of expression of the written language; recognition of this regularity is the break into the system; the mastery of this regularity is its solution." These words embrace the entire problem of the concept "cryptographic system" and likewise the task imposed upon the cryptanalyst. This is the world of his hypotheses and their collapse, of his hopes and his disappointments, of his probabilities

and of his bungling, but also of his certainties and of his art. For in spite of all factual discoveries there remains in every genuine cryptanalyst as the imponderable of his performance the "divine spark".

It must be accepted as a fact, one which may perhaps be disturbing to other peoples, that the assuring of his own existence dominates the spiritual attitude of the German to a not unessential degree. This is not the place to inquire into the causes and reasons for this attitude. The idea of serving the state all one's life is not to be separated from the idea that this state recognizes the obligation to look out for its servant when he has become old and unable to work. And the state has not tried to avoid this obligation.[55] Instead it has recognized in a decision of the Imperial High Court of Justice that the pension is merely a part of the withheld salary. If this is the norm, then it is not strange if the employee as servant of the state desires to secure for himself for his old age the return service of the state in the form of an old age pension. In the Cryptologic Bureau the cryptanalyst was an employee (Angestellter). Germany had no budgetary provision for this type of servant. Nevertheless this servant

55. The ensuing remarks should be read in connection with the following section taken from the official history of the Cryptologic Agency (probably written by FENNER) issued as DF 202: "I. Careers for Cryptanalysts:

In contrast to other countries, where an officer capable of cryptanalytic work could be active and could be promoted in this service, the German officer did not know and does not know even today of any such career. However, it had long been known that the cryptanalyst can offer a guarantee of steady performance only if he is placed in surroundings which favor his productive activity, independent of his innate qualifications. METTERNICH had endeavored to make this clear to his imperial master in a memorandum. Offering pecuniary advantages did not tally with the German conception of State service. When in 1927 the first cryptanalyst was made an official (Beamter), a development was initiated which led after long, careful preliminary work and well-planned collaboration with the administration and competent civil authorities to a 'Decree Respecting the Training and Testing for the Superior Foreign Language Service of the Armed Forces' approved by General Field Marshal KEITEL in 1939. This decree at last gave the academically trained cryptanalyst firm ground under his feet. If it freed the duly appointed cryptanalyst from uncertainty regarding his future, it also bound him as a superior official (hoeherer Beamter) closely to the national government and raised him at the same time above the numberless interpreters and translators, to whom this career remained blocked. In spite of the high demands made in all seriousness and after mature deliberation on the applicants, this decree is in a real respect the highest recognition to date of cryptanalysis".

DF 187-F

of the state in his daily life came into contact with officers and officials who were "pensionable" simply because they followed a traditional path. This was felt as an undue hardship, as an injustice which was not simply due to fate. Back in the mid-twenties some of the older cryptanalysts asked the then Director of the Cryptologic Bureau, First Lieutenant BUSCHENHAGEN, to make inquiry in competent quarters as to the circumstances under which it would be possible for the cryptanalysts to be taken over into the status of officials. The efforts of these men to get official status also had another reason. The cryptanalyst saw that the officer or official who was discharged for reasons of economy found doors of opportunity open in the economic world because his activity had not necessarily been one-sided. The man working in cryptanalysis feared, however, that in case of dismissal he might become the victim of his one-sided mental activity. This fear was not unfounded. Even METTERNICH in a memorandum to his imperial master had called to his attention the lot of his aged cryptanalysts, basing his plea on the fact that these servants of the state, who in their way were most discreet and faithful, would necessarily get into serious financial straits without a pension after a life which afforded little in the way of outward honors because their calling made it difficult for them to secure for themselves in old age any equivalent new position. In BUSCHENHAGEN's time, however, negotiations with the Ministry of Finance had no prospect of success. In 1927 I, as the constant pole of the cryptanalytic unit, became an official (Beamter) by exception; this was done to bind me permanently to the unit where the military directors changed every three or four years in any event, that is to say, just when they began to master the subject. Then for years nothing more happened until the founding of the Forschungsamt and the elevation of those employees who had left the Cryptologic Bureau to the rank of Prussian officials finally waked up the responsible officers in the Ministry of Defense and they proposed to the Ministry of Finance regular budgetary provisions for several officials and these were approved by him. Even though from a personal point of view no one could begrudge the elder cryptanalysts their promotion to Government

DF 187-F

of the state in his daily life came into contact with officers and officials who were "pensionable" simply because they followed a traditional path. This was felt as an undue hardship, as an injustice which was not simply due to fate. Back in the mid-twenties some of the older cryptanalysts asked the then Director of the Cryptologic Bureau, First Lieutenant BUSCHENHAGEN, to make inquiry in competent quarters as to the circumstances under which it would be possible for the cryptanalysts to be taken over into the status of officials. The efforts of these men to get official status also had another reason. The cryptanalyst saw that the officer or official who was discharged for reasons of economy found doors of opportunity open in the economic world because his activity had not necessarily been one-sided. The man working in cryptanalysis feared, however, that in case of dismissal he might become the victim of his one-sided mental activity. This fear was not unfounded. Even METTERNICH in a memorandum to his imperial master had called to his attention the lot of his aged cryptanalysts, basing his plea on the fact that these servants of the state, who in their way were most discreet and faithful, would necessarily get into serious financial straits without a pension after a life which afforded little in the way of outward honors because their calling made it difficult for them to secure for themselves in old age any equivalent new position. In BUSCHENHAGEN's time, however, negotiations with the Ministry of Finance had no prospect of success. In 1927 I, as the constant pole of the cryptanalytic unit, became an official (Beamter) by exception; this was done to bind me permanently to the unit where the military directors changed every three or four years in any event, that is to say, just when they began to master the subject. Then for years nothing more happened until the founding of the Forschungsamt and the elevation of those employees who had left the Cryptologic Bureau to the rank of Prussian officials finally waked up the responsible officers in the Ministry of Defense and they proposed to the Ministry of Finance regular budgetary provisions for several officials and these were approved by him. Even though from a personal point of view no one could begrudge the elder cryptanalysts their promotion to Government

DF 187-F

Councillors (Regierungsraete), nevertheless this measure did not by any means signify a basic solution of the problem of creating official positions for cryptanalysts in the regular table of organization. On the other hand, my unit was growing. Among the younger generation of cryptanalysts were a number of young university men who had already passed the first, and in some cases even the second State Examination but had not been appointed as teachers because the supply was greater than the demand. Furthermore most of them were not Party members, - consequently they would have had to sacrifice their political convictions to gain employment as teachers. In the Foreign Office conditions were similar: only the Director of the Cryptologic Bureau was an official; his cryptanalysts were employees. It is no wonder that these gentlemen could no longer conceal their concern about old age when several of my gentlemen were raised to the status of officials. The unmistakable preferential treatment of those cryptanalysts who had gone from the Cryptologic Bureau to GOERING's Forschungsamt seemed like a mockery: fidelity and loyalty to the Wehrmacht was in a way being penalized. In the matter of social position, which was so important even in the "Dritte Reich" the cryptanalysts around GOERING had therefore won their race. That not merely had an effect in small matters, e. g., in conferences with business firms, the respect with which the Cryptologic Bureau was regarded was in danger of being lost unless its cryptanalysts were given firm ground to stand on. Then late in the 30's I was instructed to draw up regulations for a career as upper grade official (hoehere Beamte) in cryptanalysis. I had thought about the matter often enough already so that the task itself was not new to me. Of course, I had to keep in mind that such a career, as career of a government official (Reichsbeamte) must be stated in such general terms that it would be valid for the Foreign Office and even for the Forschungsamt as well. The draft was worked over many times, naturally enough. For not only the Army administration was heard and consulted but also the Foreign Office and the Ministry of the Interior, the Minister of Finance, of course, and possibly even the Forschungsamt itself, which generally paid little attention to matters of government

DF 187-F

regulations. However, the Administrative Office of the Wehrmacht pushed the matter all the more vigorously. Well over a year passed before the career regulations came back into my hands with KEITEL's signature, approved as in the draft. But with that an almost twenty-year-old struggle was ended and we had firm ground under our feet.

The most important points in the career regulations were:

1. Creation of the officials of the "Superior Foreign Language Service of the Armed Forces."
2. Applicants. Basically eligible are only university trained men who have the doctorate or have passed the first major State Examination.

Admitted are: philologists, jurists, mathematicians and natural scientists with full mastery of one foreign language and a good knowledge of a second foreign language. Mathematicians need show a knowledge of only one foreign language. As a normal requirement a clean record was demanded, and in the case of applicants who wished to enter the Wehrmacht physical fitness and, if possible, evidence that they had completed their period of service in the Army. Before being accepted the applicant had to submit to an examination in which he was to prove his linguistic knowledge or his mathematical knowledge. If the results of the examination were favorable, he was given a provisional appointment as regular or supernumerary Regierungsassessor (according to whether a position was vacant or not). (The type of examination corresponded to the one I have described above).

3. Training. Assignment of tasks was as in the case of any beginner but with the difference that the section head, to whom an "Assessor" was assigned for training, was to present every three months a report on the [illegible]ties with remarks as to his suitability. The applicant himself was to keep a record of his activities and present it monthly. The applicant must have attended the course in lower cryptology with demonstrable success (two years). After the expiration of three years (total time) at the earliest, the applicant might apply for admission to the second major state examination with the purpose of being accepted as lifelong official of the

DF 187-F

Superior Foreign Language Service of the Armed Forces (- cryptanalyst). Admission to the examination was only granted as a matter of principle if the appropriate section head and the director of the cryptanalytic unit were of the opinion that the examinee had mastered the material and was sufficiently mature. (To the regular training of the applicant belonged also lectures on the Civil Service Law, Organization of the Wehrmacht, Patent Law and Disciplinary Law).

4. Examination. First day: Translation into German of some 20 lines of a foreign article on cryptography or cryptology (written). Examination of a simple cryptographic system, e. g., of a linear slide or disc system or some similar gadget. Solution of a basic system by analysis with a criticism. (Instead of this assignment mathematicians were given a problem from cryptologic mathematics). Time: 6 hours.

Second day: Approximately 20 minutes devoted to a test on law, then about 50 minutes on cryptography and cryptology. Not more than three examinees at the same time.

5. Examining Commission. The Chief of the Cryptologic Bureau, the Director of the cryptanalytic unit and one of the teachers who had participated in the training, and a representative of the Administrative Office of the Wehrmacht.

6. Results of the examinations. The Commission rated the performances according to nine grades from "Deficient", to "Laudable". Since none of the candidates desired to become administrative officials with legal duties, in the rating one point was added to the rating in law before the average was taken. If two candidates had equally good ratings the preference was given to the one whose bearing during the examination was better and who was con- [illegible] the higher character.

7. If a candidate did not pass the examination, he was given the option of repeating the examination in a year. A third examination was forbidden.

8. Applicants who passed the examination were appointed Government Councillor (Regierungsrat) and received corresponding salaries and secured the right to the old age pension and provision for widows established by law. The officials were permitted as officials of the Wehrmacht to wear the uniform of

the branch of the service selected and took the prescribed oath of office.

A further provision took account of the circumstance that there was as yet no experience to show whether the requirements covered in the examination could be met in the prescribed time. Therefore amendments were to be possible and were to be worked out in agreement with the examining commission and the agencies involved, e. g., elimination of certain juristic questions, extension of the time for solving the cryptologic problem. The intention was to avoid a rigid scheme which would not correspond to the actual demands of the profession. There was further provision that only those officials should be allowed to wear a uniform who had fulfilled their obligation to serve in the Wehrmacht in order to avoid having an official who was regarded by the people as an officer - only an expert could distinguish an officer's uniform from an official's uniform - giving occasion for adverse criticism.

In my opinion the career regulations had a beneficial effect. Order was secured and there was a clear understanding as to who had a legal claim to become an official and who did not. Wild claims could no longer be made which were based on the more or less subjective impression of a man who was trying to represent the unfairness of his superiors as the sole cause of his personal failure. And those officials who were appointed or promoted after having passed an examination had the moral satisfaction of not having become officials due to some dubious favor but after honest proof of their ability by satisfying recognized requirements.

The examination was by no means "pro forma" but demanded proof of actual knowledge of the subject and a knowledge which could be turned to account at any time. Both parties, the examiner and the examinee, were expected to show great po[illegible]tion. The preparation of the various examinations took weeks of effort since, despite the difference in their appearance and content, they all had to be approximately equal in difficulty. The conscientious observance of all regulations and prescribed authority called for an exact acquaintance with the subject and the actual responsibility lay nevertheless on the shoulders of the head of the cryptanalytic section, which, however, was a matter of course in view of the importance of the examination.